

Implementation Plan
For the
Information Sharing Environment
Electronic Directory Services –
People & Organizations

March 21, 2006

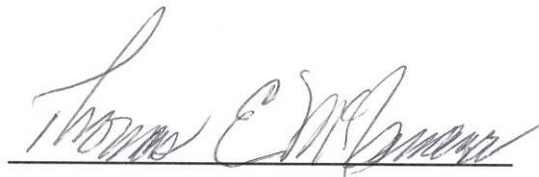
UNCLASSIFIED

ISC Document
No. 0002

INFORMATION SHARING COUNCIL
WASHINGTON, DC 20511

FOREWORD

1. The Implementation Plan for the Electronic Directory Services – People & Organizations (EDS-PO), an Information Sharing Council (ISC) sponsored component of the Information Sharing Environment (ISE), defines governance, development and deployment strategies for the EDS-PO Phases 1 and 2. Future Phases (after Phase 2) are not covered in this document. The Implementation Plan, with the March 21, 2006 approval of the ISC, will continue to be revised and updated based on new and emerging user requirements.
2. Representatives of the Information Sharing Council may obtain additional copies of this CONOPS at the address listed below.
3. U.S. Government contractors and vendors shall contact their appropriate government agency or Contracting Officer Representative regarding distribution of this document.



Thomas E. McNamara
Chair, Information Sharing Council
Program Manager, Information Sharing Environment

ISC Secretariat, 2100 K St., NW, Washington, D.C. 20511
(202) 331-4060 FAX: (202) 296-5545
ISC_Secretariat@dni.gov

UNCLASSIFIED

Table of Contents

EXECUTIVE SUMMARY	V
1 INTRODUCTION.....	1
1.1 DOCUMENT SCOPE	1
1.2 GAP ANALYSIS	2
2 GOVERNANCE, ROLES AND RESPONSIBILITIES	5
2.1 PROGRAM MANAGER, INFORMATION SHARING ENVIRONMENT	5
2.2 INFORMATION SHARING COUNCIL	6
2.3 IMPLEMENTATION AGENT	6
2.3.1 Selection Criteria	7
2.3.2 Selection Process	7
2.3.3 Roles and Responsibilities	7
2.4 MISSION VALIDATION TEAM	8
2.4.1 Selection Criteria	8
2.4.2 Roles and Responsibilities	8
2.5 IMPLEMENTATION COORDINATION TEAM	9
2.5.1 Selection Criteria	9
2.5.2 Roles and Responsibilities	9
2.6 SYSTEM OWNER	9
3 PHASE 1 IMPLEMENTATION	10
3.1 PHASE 1 APPROACH	10
3.2 PHASE 1 SCOPE	10
3.3 PHASE 1 TIMELINE	11
3.4 PHASE 1 TASKS	11
3.4.1 Select the Implementation Agent(s).....	11
3.4.2 Data Call	11
3.4.3 Develop and Populate Blue Page	12
3.4.4 Publish Blue Page	12
3.4.5 Provide Data Update Capability	12
3.4.6 Provide User Feedback Mechanism.....	12
3.4.7 Develop Customer Outreach Plan	12
3.4.8 Develop Phase 2 Implementation Plans.....	13
3.5 PHASE 1 DELIVERABLES	13
4 PHASE 2 IMPLEMENTATION	14
4.1 PHASE 2 APPROACH	14
4.2 PHASE 2 SCOPE	14
4.3 PHASE 2 TIMEFRAME	14
4.4 PHASE 2 TASKS	14
4.4.1 Select Implementation Agent(s)	14
4.4.2 Develop Implementation Plan and Estimates	15
4.4.3 Enhance Phase 1 Initial Capability	15
4.4.4 Integrate Additional Data Sources	15

UNCLASSIFIED

4.4.5	Increase Data Population	16
4.4.6	Integrate Existing Capabilities	16
4.4.7	Introduce Yellow Pages	16
4.4.8	Introduce Blue Page Dynamic Update.....	16
4.4.9	Introduce Blue Page on the SBU Domain	16
4.4.10	Enhance USBLUEPAGES.GOV	16
4.4.11	Phase 2 Deliverables	16
5	CONCLUSION	17
	GLOSSARY AND ACRONYMS	18
	APPENDIX A – PHASE 1 TASK LIST.....	20
	APPENDIX B – HIGH LEVEL ROLES AND RESPONSIBILITIES	21
	APPENDIX C – DATA MANAGEMENT & QUALITY ASSURANCE	22

List of Tables

TABLE 1: EDS-PO SCOPE BY PHASE.....	1
TABLE 2: SCI EXISTING SYSTEMS	2
TABLE 3: SECRET EXISTING SYSTEMS	3
TABLE 4: SBU EXISTING SYSTEMS.....	3

List of Figures

FIGURE 1: IMPLEMENTATION GOVERNANCE	5
FIGURE 2: PHASE 1 TIMELINE	11

UNCLASSIFIED

Executive Summary

The Implementation Plan defines governance, development and deployment strategies for the Electronic Directory Services – People & Organizations (EDS-PO), an Information Sharing Council (ISC) sponsored component of the Information Sharing Environment (ISE). The Approach, Scope, Deliverables, Timeline and Tasks for EDS-PO Phases 1 and 2 are defined herein. The Implementation Plan builds upon the EDS-PO Concept of Operations approved by the Program Manager, ISE on February 22, 2006. Future Phases (after Phase 2) are not covered in this document.

The Implementation Plan defines criteria for selecting the Implementation Agent (IA) – the organization responsible for the development and deployment of an EDS-PO system in a specific network security domain. Roles and responsibilities for the ISE Program Manager (PMISE), the ISC and the IAs are also defined.

The EDS-PO Phase 1 details are fully defined in this document. EDS-PO Phase 1 will be completed by March 31, 2006 and will recognize existing EDS-like capabilities as well as provide an initial "Blue Page" webpage for Counterterrorism-related organizations within the SCI and SECRET network security domains. Additionally, the IAs will complete detailed Implementation Plans for the Phase 2 implementation within their assigned security domain and submit estimates for cost and resources to the PMISE by April 14, 2006 for ISC review.

The EDS-PO Phase 2 implementation will provide enhanced Phase 1 capability and introduce new functionality. Certain EDS-PO Phase 2 details are To Be Determined (TBD), depending on future decisions by the ISC and PMISE. Currently, EDS-PO Phase 2 is scheduled to be completed by March 31, 2007 and will include further enhancement to the Blue Page, expansion of data sources and utility to the existing White Pages and the definition and introduction of the Yellow Pages.

1 Introduction

Section 1016 of the Intelligence Reform and Terrorism Prevention Act (IRTPA) calls for improved sharing of terrorism information to support the country's ability to effectively prosecute the Counterterrorism (CT) mission.¹ Improved sharing of information allows users to more efficiently and effectively locate, interact and connect the dots with their counterparts in other government agencies.

The PMISE approved the Concept of Operations (CONOPS) for the Electronic Directory Service - People and Organizations (EDS-PO) on February 22, 2006. The EDS-PO CONOPS, developed under the direction and guidance of the PMISE and the ISC, provides a description of the required functionality of the EDS-PO and serves as the guiding document for the Implementation Plan. EDS-PO implementation is governed by the PMISE, with the advice of the ISC.

1.1 Document Scope

This document defines the approach and governance for the phased EDS-PO implementation to meet the requirements as specified in the EDS-PO CONOPS. The Implementation Plan identifies selected systems that already provide some or all of the services and functionality required for the EDS-PO and provides a detailed Task list for Phase 1 implementation and high-level guidance to the IA for Phase 2 implementation.

The following table summarizes the scope of the EDS-PO Phase 1 and Phase 2 implementations:

Phase 1	First priorities in Phase 1 are the implementation of a web-based Blue Page directory and identification of current capabilities that support the EDS-PO CONOPS. Deliverables include manually constructed and updated Blue Page on the SCI and SECRET network security domains, user feedback mechanisms, links to existing systems that provide EDS-PO functionality, user outreach plan and a Phase 2 Implementation Plan. A nominal resource commitment will be necessary from the hosting provider. Phase 1 will be completed by March 31, 2006.
Phase 2	Begin the integration of additional directory sources into selected White Pages systems. Introduce and incrementally develop a Yellow Page capability. Enhance the functionality and dynamic update capability of the Blue Page to better utilize the expanding White Pages capabilities. The funding source and mechanism are not yet determined. Phase 2 consists of incremental enhancements to the IOC capability and will be completed by March 31, 2007.
Future Phases	Guided by the ISE CONOPS. Integration of the EDS-PO functionality into the Information Sharing Environment (ISE) Services Oriented Architecture (SOA) framework. Continue the enhancement of Phases 1 and 2 capabilities.

Table 1: EDS-PO Scope By Phase

Specifically, Section 2 of this document defines the governance, roles and responsibilities of the key stakeholders for EDS-PO. Section 3 provides a detailed description of the

¹ Pub. L. No. 108-458, 118 Stat. 2638 (Dec. 17, 2004) [hereinafter IRTPA].

UNCLASSIFIED

Phase 1 timeline, tasks and deliverables, as well as the high level scope and deliverables of Phase 2.

1.2 Gap Analysis

The EDS-PO Implementation Team conducted a data call to identify existing systems that meet some or all of the functionality as specified in the EDS-PO CONOPS. The response to the data call indicates that many of the existing systems provide some directory services to their specified user base. A few of the existing systems provide Blue Page type contact information for CT-related organizations and several systems provide White Pages-like access across multiple agencies.

However, most of the existing systems are either accessible to only a subset of users on its host network security domain, contain a small subset of user directory information or require a user account for access. Some systems, such as the Analyst Yellow Pages portion of the Analytic Resource Catalog (ARC) provide some Yellow Page functionality.²

Each of the following tables contain systems that were identified as having some directory functionality in the SCI, SECRET and Sensitive But Unclassified (SBU) network security domains.

	SCI Security Domain Systems	Current Sharing Initiatives	Owner	EDS-PO CONOPS Functionality			Comments
				White	Yellow	Blue	
1	IC Full Services Directory (IC FSD)	X	DNI	X			Name lookup, some additional functionality if fields are populated by System Owners
2	Intelink	X	DNI	X	X	X	Organization points of contact, web pages, Google, Info Work Space, IC Instant Messaging, content differs by agency
3	Analytical Resource Catalog (ARC)	X	DNI	X	X		Provides skill related attributes
4	NCTC Online (NOL)	X	NCTC	X	X	X	CT-community relevant info, requires account+PKI+HCS clearance

Table 2: SCI Existing Systems

² The ARC expresses the intelligence expertise of analysts by applying a National Intelligence Priorities Framework Intelligence Topic and identifying their organization. While not a specific organizational list of services, as you would find in a Yellow Page listing, services can be inferred by expertise.

UNCLASSIFIED

	Secret Security Domain Systems	Current Sharing Initiatives	Owner	EDS-PO CONOPS Functionality			Comments
				White	Yellow	Blue	
1	IC Full Services Directory (IC FSD)	X	DNI	X			Name lookup, some additional functionality if fields are populated by System Owners (when available in SECRET domain)
2	Intelink	X	DNI	X	X	X	Organization points of contact, web pages, Google, content differs by agency
3	Global Address Lists	X	DOJ FBI	X			Within DOJ and FBI
4	Active Directory		DOS	X			Authentication directory
5	DOS Web Phone Directory		DOS	X		X	
6	NCTC Online (NOL)	X	NCTC	X	X	X	CT-community relevant info, requires account

Table 3: SECRET Existing Systems

	SBU Security Domain Systems	Current Sharing Initiatives	Owner	EDS-PO CONOPS Functionality			Comments
				White	Yellow	Blue	
1	Directory Services and Email Systems (DSES)		DHS	X			Directory service internal to DHS
2	Cyber Identity Management (CIM)		DHS	X			Designed to federate with non-DHS services
3	Global Address Lists	X	DHS DOJ	X			Bridges DOJ and DHS
4	Intelink	X	DNI	X	X	X	Organization points of contact, Google
5	LEO Directory	X	DOJ FBI	X			CT-related situational awareness and collaboration across wider CT community
6	National Criminal Intelligence Resource Center	X	DOJ	X	X	X	Ready for deployment
7	RISS Directory		DOJ	X			Contact info for SLT law enforcement ³
8	Active Directory		DOS	X			Authentication Directory
9	DOS Web Phone Directory		DOS	X		X	
10	E*Phone		DOS	X			DOS only
11	US P3	X	FBI	X	X	X	Multiple US regions
12	NCTC Online (NOL)	X	NCTC	X	X	X	Requires account, limited partners; less functionality than SCI and SECRET domains
13	HR Connect		Treas	X			

Table 4: SBU Existing Systems

³ SLT refers to State, Local and Tribal entities.

UNCLASSIFIED

UNCLASSIFIED

To address the shortfalls identified in the data call the EDS-PO will:

- Provide a consolidated view of contact information for CT-related organizations;
- Provide a point of access to existing systems;
- Expand the data sources of existing systems;
- Introduce new capabilities in the form of Blue Pages and Yellow Pages; and
- Provide a functional roadmap toward the EDS service within the ISE.

UNCLASSIFIED

2 Governance, Roles and Responsibilities

Managing the implementation efforts to meet CONOPS-specified capability requirements requires coordination across all participating Departments and Agencies. Figure 1 depicts a governance structure designed to ensure all key participants are involved.

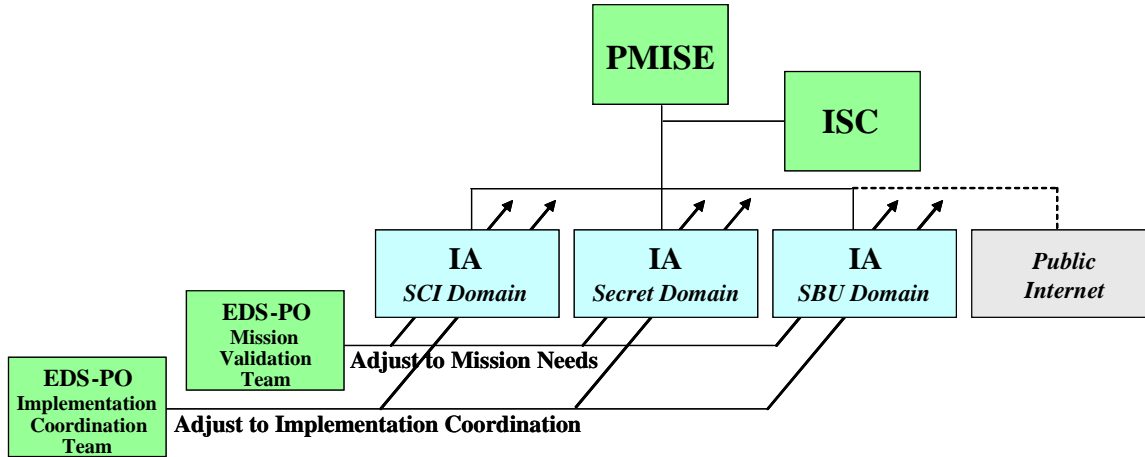


Figure 1: Implementation Governance

Primary players are the PMISE, ISC, IAs and teams supporting mission validation and implementation coordination.

The IA is responsible for overall guidance and direction of implementation efforts within the constraints of the EDS-PO CONOPS and Implementation Plan. However, feedback and involvement from participating organizations is necessary to ensure success. Therefore, a Mission Validation Team (MVT) will be established to provide feedback and a basis for adjustments to CONOPS-specified capability requirements and the Implementation Coordination Team ensures the detailed implementation strategies are viable. The IA will perform adjudication of differences.

2.1 Program Manager, Information Sharing Environment

Per IRTPA, the Program Manager, Information Sharing Environment (PMISE) will have and exercise government-wide authority regarding the ISE. Applying this authority to EDS-PO, the PMISE will:

- Serve as the Executive Agent (EA) to oversee and have ultimate responsibility for the implementation and management of the EDS-PO;
- Develop policies, procedures, guidelines, rules and standards as appropriate to foster the development and proper operation of the EDS-PO;
- Monitor and assess the implementation of the EDS-PO by Federal departments and agencies to ensure adequate progress, technological consistency and policy compliance;

UNCLASSIFIED

- Prepare the EDS-PO Implementation Plan and obtain ISC concurrence for the plan;
- Identify potential EDS-PO Implementation Agents. Select EDS-PO Implementation Agents with the advice and consent of the ISC;
- Arrange with MVT members for pre-deployment reviews and/or prototype hands-on demonstrations;
- Validate that EDS-PO CONOPS requirements have been met; and
- Generate future iterations/evolutions of the CONOPS and Implementation Plan. Supervise the IAs, the MVT and the Implementation Team to ensure lessons are captured to influence those iterations/evolutions.

2.2 Information Sharing Council

The Information Sharing Council (ISC) will:

- Advise the PMISE in developing policies, procedures, guidelines, roles and standards necessary to establish, implement and maintain the EDS-PO;
- Work to ensure coordination among the Federal departments and agencies participating in the EDS-PO in the establishment, implementation and maintenance of the EDS-PO;
- Review and provide concurrence or non-concurrence to the PMISE regarding approval of the EDS-PO CONOPS;
- Review Implementation Plans developed by the IAs;
- Review and provide concurrence or non-concurrence to the PMISE regarding appointment of Implementation Agents; and
- Advise the PMISE regarding validation that EDS-PO CONOPS requirements have been met.

2.3 Implementation Agent

The Implementation Agent (IA) will ensure implementation efforts meet specified functionality and phased deliveries in support of EDS-PO CONOPS-identified capabilities within the applicable network security domain. The IA is the senior government official that leads the organization selected using the criteria set forth below.

UNCLASSIFIED

2.3.1 Selection Criteria

An IA must:

- Have extensive knowledge and experience with web-based services and applications in the appropriate network security domain;
- Have a record of success in establishing cross-organizational web-based services;
- Have development, contracting, operations and maintenance infrastructure available to support required workload; and
- Have an existing information technology governance structure that can integrate EDS-PO into its portfolio.

2.3.2 Selection Process

The Implementation Team will identify potential candidates, assess them against the criteria in Section 2.3.1 and recommend an IA to the PMISE and ISC. The ISC representative will verify that selection criteria have been met for each IA candidate organization.

2.3.3 Roles and Responsibilities

For Phase 2, the IA task was separated into planning and execution roles. The IAs selected for the planning stage may be different for those selected for the execution stage.

The Planning IA will:

- Develop detailed Phase 2 Implementation Plan for their respective security domain;
- Provide cost and resource estimates derived from the development of the Implementation Plans. These are due to the PMISE by April 14, 2006;

The Execution IA will:

- Ensure technical integration of solution set components;
- Coordinate with network owners/operators to set expectations for load planning, applicability of existing agreements and adjustments, as necessary;
- Coordinate programming, budgeting and funding amongst system owners and the PMISE;
- Recommend policies and standards as required to enable implementation and ensure consistency among the three security domains;

UNCLASSIFIED

- Ensure ISC standards, policy and guidance are followed; ensure compliance for any operating or maintenance standards established for EDS-PO;
- Establish schedules and lead execution to deliver EDS-PO CONOPS-directed capabilities within PMISE-established timelines;
- Report implementation status to the PMISE;
- Coordinate with MVT representatives to arrange pre-deployment reviews and/or prototype hands-on demonstrations;
- Coordinate with other network security domain IAs to maximize the sharing of information and ensure that efforts do not diverge;
- Assess performance to EDS-PO CONOPS-specified capability requirements and report to the PMISE; and
- Apply programmatic rigor based on standard program management practices to the development and operation of the EDS-PO.

2.4 Mission Validation Team

A Mission Validation Team (MVT) of user representatives will be a primary mechanism for providing focused user feedback. User feedback is essential to ensure EDS-PO Phases 1 and 2 meet CONOPS-specified capability requirements and that future evolutions of EDS-PO maximize customer utility. Periodically, the IA will recommend to the PMISE that the MVT be used to provide feedback and inputs to EDS-PO evolution on an ad hoc basis.

2.4.1 Selection Criteria

User representatives must be users or user supervisors that are directly involved in CT analysis, operations or activity that would benefit from EDS-PO. Each participating organization should be represented by two users; one Watch Center employee and one Analyst.

2.4.2 Roles and Responsibilities

Mission Validation Team members will:

- Validate for the PMISE that EDS-PO CONOPS-specified end-user capability requirements have been met;
- Participate periodically in pre-deployment reviews and/or hands-on demonstrations of EDS-PO prototypes;
- Recommend “Go Live” to the ISC for functional initiations and enhancements;
- Respond periodically to user surveys issued by the IA; and
- Support PMISE efforts to define capability requirements for future iterations/evolutions of EDS-PO.

UNCLASSIFIED

2.5 Implementation Coordination Team

Participating organizations will be involved in planning and execution of EDS-PO implementation through the Implementation Coordination Team.

2.5.1 Selection Criteria

In order to ensure leverage of existing systems, application/adaptation of significant lessons learned and viability of proposed solutions, Implementation Coordination Team members will ideally possess information technology, programmatic, technical and security expertise.

2.5.2 Roles and Responsibilities

The Implementation Coordination Team will:

- Maintain cognizance of participating organization directory services and related initiatives in order to recommend potential points of synergy to the IA (for current phase) and PMISE (for future phases);
- Advise the IA on potential program benefits and impacts to their organizations from proposed implementation strategies and solutions;
- Identify barriers to implementation within respective organizations and recommend approaches to remove those barriers; and
- Ensure that information security requirements are maintained consistent with applicable Agency policies.

2.6 System Owner

Each owner of an existing system to which the EDS-PO capabilities will be linked as part of the solution set will be responsible for detailed implementation with respect to the owned system. This will also include:

- Programming, planning and budgeting for integration and necessary enhancement;
- Assessment and reporting of implementation status through the IA to the PMISE; and
- Participation in and support to the Mission Validation Team to verify that EDS-PO CONOPS-specified capability requirements are met.

3 Phase 1 Implementation

3.1 Phase 1 Approach

Phase 1 will provide a capability that allows users to find organizations in the SCI and SECRET network security domains that have terrorism information and responsibilities. The approach will utilize the functionality of existing systems by providing easy navigation to those systems, as well as provide an initial web-based Blue Pages (organizational contact information) capability.

3.2 Phase 1 Scope

Phase 1 will:

- Initiate formation of an ISE Blue Page capability that allows user to identify and contact terrorism related organizations operating on the SCI and SECRET network security domains;
- Provide a central point of access to existing systems that can provide a best effort portion of the information described in the EDS-PO CONOPS;
- Select a location to host the Blue Page; and
- Ensure Blue Page information is kept up to date by responding to feedback on updates as well as performing periodic quality audits.

Prior to Phase 1, the PMISE, with advice of the ISC, will designate an Implementation Agent (IA) who will lead the development of a detailed Implementation Plan for each of the SCI and SECRET network security domains for Phases 1 and 2 implementations. Phase 1 will be complete when the initial operating capability (IOC) of EDS-PO is articulated key stakeholders and users as defined by the EDS-PO CONOPS.

3.3 Phase 1 Timeline

The Phase 1 timeline runs from the date the EDS-PO Implementation Plan is approved until March 31, 2006. The IOC will be successful if requirements below are met and the MVT certifies that the EDS-PO IOC provides value-added functionality to the CT community, as determined by the March 31, 2006 deadline.

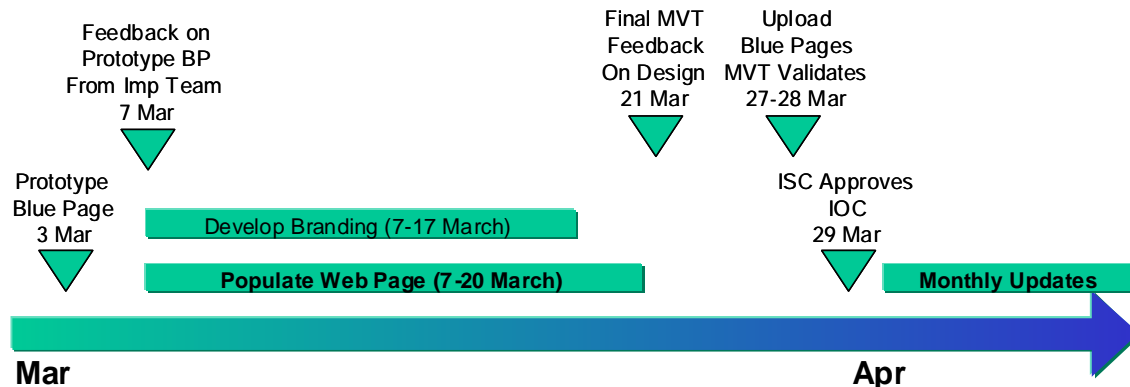


Figure 2: Phase 1 Timeline

3.4 Phase 1 Tasks

3.4.1 Select the Implementation Agent(s)

The PMISE, with the advice and consent of the ISC, will select an IA for each of the SCI and SECRET network security domains. The IA may be the same for each security domain.

3.4.2 Data Call

The PMISE will conduct a data call to capture necessary data for development of the Blue Page. The response to the data call will include all available “mandatory” and “provide if available” attributes, as defined by the CONOPS, for each organization. PMISE will develop the data call for approval of the ISC. The data call results will:

- Include contact information for at least one CT related organization (if available) for each of the EDS-PO participants with attributes as currently assigned in either National Intelligence Priorities Framework (NIPF) Intelligence Topics (IT) or other attributes as determined by the EDS participant; and
- Success criteria: Threshold data-set with at least 8 ISC represented organizations and MVT concurrence.

3.4.3 Develop and Populate Blue Page

IA will develop an ISE Blue Page (webpage) and populate with the data received through the data call. The Blue Page site will:

- Be a webpage that is a list of organizations. NIPF ITs and other (see Task 3.5.2) criteria will be displayed with the Organizational contact information. The Organization Name will contain a link to their homepage on that network, if available.
- Success criteria: Threshold webpage with MVT concurrence.
- Contain a link (URL) to systems that already provide some EDS-PO functionality, defined by the selection criteria (See Section 1.2 *Gap Analysis*.)
- Success criteria: Threshold listing of links with MVT concurrence.

3.4.4 Publish Blue Page

IA will select a location (URL) and publish the ISE Blue Page on the SCI and SECRET network domains. The published ISE Blue Page will:

- Be published to a site that is viewable to all users that have access to that network security domain; and
- Success criteria: an operational Blue Page capability with data provided by eight or more ISC member organizations; successful security and legal review; and MVT validates functionality and recommends “Go Live.”

3.4.5 Provide Data Update Capability

IA will provide a mechanism and business rules for EDS-PO data providers to maintain the accuracy of their data posted to the Blue Page. The update/correction mechanism will:

- Be a monthly update with minimal effort requirements on the IA;
- Success criteria: IA deploys a method of keeping information current and accurate with the functionality stated above.

3.4.6 Provide User Feedback Mechanism

IA will provide a user feedback mechanism to capture information used for further enhancements to content and functionality. The feedback mechanism will:

- Be a periodic meeting of the MVT under the auspices of the PMISE.

3.4.7 Develop Customer Outreach Plan

The PMISE, in conjunction with the IA, will develop an Outreach Plan to address the marketing and training aspects of providing the new EDS-PO capabilities.

3.4.8 Develop Phase 2 Implementation Plans

The IA will develop Implementation Plans for the initial Phase 2 enhancements to meet the operational requirements in the CONOPS. Initial Phase 2 enhancements will be to enhance the EDS-PO requirements in Section 4.4.3. Additionally, because suggested enhancements to functionality generated by user feedback and the MVT may be prioritized to implement in Phase 2, the IA will develop a process to include those enhancements into the implementation schedule.

3.5 Phase 1 Deliverables

- Selection of an IA for each network security domain;
- Blue Page directory capability on the SCI and SECRET network domains;
- A capability to report usage statistics and a mechanism for user feedback (see section 3.5.6 and CONOPS section 4.2.3);
- Links from the Blue Page to existing systems that provide EDS-PO functionality on the two network security domains;
- Phase 2 Implementation Plans for the SCI and SECRET network domains due April 14, 2006;
- User Outreach Plan to promote user-awareness of additional capabilities (see CONOPS section 4.3.1); and
- Blue Page Data Quality Assurance Plan.

4 Phase 2 Implementation

4.1 Phase 2 Approach

The Phase 2 approach is to enhance the threshold capabilities developed in Phase 1 to meet all Phase 2 requirements defined in Section 4.4.3. Additionally, the IA will begin the implementation of the prioritized list of requirements derived from the CONOPS through the execution of the network level Implementation Plans. Funding and resources will be estimated through a process led by the IA and coordinated with the PMISE as the Phase 2 increments become better understood. Phase 2 estimates will be complete by April 14, 2006, so that funds and resources can be identified for implementation. The PMISE will keep the IA apprised of developments and status of the ISE CONOPS to minimize divergent development. Phase 2 may be re-scoped to meet the requirements laid out in the developing ISE CONOPS or by the MVT, as necessary. Phase 2 represents the incremental improvement to the IOC capabilities over the next 9-12 months.

4.2 Phase 2 Scope

Phase 2 is the incremental increase in capability to meet the requirements in the EDS-PO CONOPS. The selected core systems from Phase 1 that provide some of the requirements and functionality will be enhanced by adding additional participants to the portfolio, as well as expanding functionality to the user interface. Additionally, the initial Yellow Page capability will be defined and introduced.

4.3 Phase 2 Timeframe

The Phase 2 timeframe will begin April 1, 2006 and continue through March 31, 2007. Phase 2 is broken down into Planning and Execution phases. The planning phase includes the development of a detailed Implementation Plan that includes detailed cost and resource estimates. The Plan and estimates are due to the PMISE by April 14, 2006 for consideration by the ISC. The Execution phase will begin once the plan and cost estimates are approved.

4.4 Phase 2 Tasks

4.4.1 Select Implementation Agent(s)

The PMISE, with the advice and consent of the ISC, will select an IA for each of the SCI and SECRET network security domains. The IA may be the same for each security domain and may change following the Planning Phase (see Section 4.4.2).

4.4.2 Develop Implementation Plan and Estimates

Phase 2 is broken down into a Planning Phase and an Execution Phase (summarized below). The Planning Phase, beginning upon selection of the IA(s), will end with the approval of a detailed Implementation Plan with the scope and strategy for Phase 2 implementations and a cost and resources estimate. The Plan and estimates are due to the PMISE April 14, 2006 for consideration and approval by the ISC. The ISC may select a different IA for each domain based on resource and funding constraints identified during the Planning Phase.

The Execution Phase begins upon ISC approval of the detailed Implementation Plans, the selection of the execution IA(s) and concludes March 31, 2007.

- Planning Phase – Develop detailed Implementation Plan with cost and resource estimates by April 14, 2006
- Execution Phase – Upon ISC approval, execute the details of the Implementation plan through March 31, 2007.

4.4.3 Enhance Phase 1 Initial Capability

IA will enhance all Phase 1 capabilities to meet the following requirements (as specified in Section 3.5 of the Implementation Plan):

- Section 3.5.2-in addition to Threshold, include all federal and interagency level CT related organizations with full contact information and search criteria.
- Section 3.5.5-in addition to Threshold, be an on-demand capability where EDS-PO data providers can update the Blue Page whenever necessary to maintain the accuracy of their contact information.
- Section 3.5.6-in addition to Threshold, be integrated into the Blue Page as an optional activity of the user.
- Section 3.5.3-enhance the Blue Page to be a display of organizations that are searchable by a subset of NIPF ITs and/or attributes provided by data providers in Section 3.5.2. Only those attributes that are tied to an organization will be searchable. The Organization Name will contain a link to their homepage on that network, if available. Each entry will include two date/time stamps, if available, for “last updated” and “last reviewed.”
- Section 3.5.3-integrate search functionality of linked systems into the Blue Page.

4.4.4 Integrate Additional Data Sources

IA will integrate additional data identified in the Gap Analysis (Section 1.2.) Using existing governance and standards, links to additional directories will be incrementally added as they become available on both the SCI and SECRET domains.

4.4.5 Increase Data Population

Under the technical direction of the IA and in accordance with internal policies and procedures, data providers to existing directory services will populate the existing fields in their directories to the greatest extent possible, on both the SCI and SECRET domains.

4.4.6 Integrate Existing Capabilities

IA will work with the ARC and IC FSD owners to integrate ARC and IC FSD search functionality into the Blue Page to better utilize White Page information available in the IC FSD.

4.4.7 Introduce Yellow Pages

PMISE and IA will define the “services” that will constitute the Yellow Pages and then introduce and incrementally enhance a Yellow Page capability into the Blue Page. Yellow Page type services will be mapped to organizations listed on the Blue Page.

4.4.8 Introduce Blue Page Dynamic Update

IA will introduce and incrementally enhance dynamic updates of the Blue Page information.

4.4.9 Introduce Blue Page on the SBU Domain

IA will select a location and deploy the Blue Page for the SBU domain.

4.4.10 Enhance USBLUEPAGES.GOV

PMISE and IA will develop a plan and implement the enhancement of USBLUEPAGES.GOV with appropriate CT-related organizational information for use on the public Internet.

4.4.11 Phase 2 Deliverables

5 Conclusion

Successful implementation of Phases 1 and 2 will provide initial capabilities to help start users in transition to new levels of information sharing. User lessons fed back to the PMISE and ISC will be critical to defining the future evolution of EDS-PO, as well as provide important inputs to the establishment of the full ISE.

Glossary and Acronyms

Attributes: Specific data entries associated with people and organizations. Such data entries will perform one or more of the following functions:

- Identify people or organizations
- Provide search characteristics
- Enable management of the EDS-PO

Counterterrorism (CT): The practices, tactics and strategies that governments, militaries and other groups adopt in order to neutralize terrorist operatives in the U.S. and to dismantle terrorist networks worldwide.

Current Capabilities Matrix: Spreadsheet of directory systems currently in operation, development, or planned within the Federal sector.

Data Quality Representative: An individual from each participating organization who is the primary point of contact with the PMISE regarding data management. The representative ensures that their organization's directory information is accurate and current.

Electronic Directory Services – People & Organizations (EDS-PO): A set of registries that share a common, trusted and up-to-date view of people and organization information, which includes identification of necessary attributes, desired attributes and standardized metadata on people and organizations, to assist in locating in the Federal Government people with relevant knowledge about intelligence and terrorism information.

Information Sharing Council (ISC): The ISC is an interagency forum established by Section 1016 of IRTPA and Executive Order 13388 and operating under a Charter approved by the ISPCC. It is an advisory body to the President and PM in the development of policies, procedures and guidelines necessary to implement the ISE. Additionally, it provides participants an avenue to actively engage in implementation planning and decision-making for the establishment of an effective ISE. The Council also acts as a mechanism to ensure coordination among Federal departments and agencies and is a means for the PM to assess progress among ISE communities. The ISC was recently directed to establish two sub-committees to address State, Local and Tribal as well as private sector issues. These subcommittees will be co-chaired by DHS and DOJ.

Information Sharing Environment (ISE): an approach that facilitates the sharing of terrorism information, which approach may include any methods determined necessary and appropriate for carrying out this section.

Information Sharing Policy Coordination Committee (ISPCC): Established by the President in June, 2005, the ISPCC is chaired jointly by the Homeland Security Council (HSC) and the National Security Council (NSC). It has the responsibilities set forth in Section D of Homeland Security Presidential Directive 1 and other relevant

UNCLASSIFIED

presidential guidance with respect to information sharing. The ISPC was established to address major information sharing policy issues, including the resolution of issues raised by the PM and provide policy analysis and recommendations for consideration by the more senior committees of the HSC and NSC systems.

Mission Validation Team: Participating organization representatives that provide focused user feedback.

Private Sector (PS): Non governmental organizations such as commercial and academic entities.

Program Management Office (PMO): Staff supporting the Program Manager. The PM's Office is supported by an experienced staff from across the U.S. Government. Supporting personnel include several advisors with expertise in specific information sharing issues, e.g., State and Local information sharing and technology standards.

Program Manager: The PM will build upon current information sharing efforts across the U.S. Government and facilitate change toward tomorrow's ISE, engaging the ISC in the implementation process through continuous communication, interaction and inclusion in decision-making processes. The PM will act as the catalyst to improve terrorism information sharing among ISE communities by working with them to remove barriers and facilitate change to improve information access.


Sharing Initiatives Matrix: Spreadsheet of directory systems currently in operation within the Federal sector which provide information across organizational lines.

Stakeholder: The EDS-PO principal stakeholders are those organizations that will provide their directory information to the EDS-PO.

State, Local and Tribal (SLT): Non-Federal public sector, including government, police, justice and health and human services, that are involved in or could be impacted by CT.

UNCLASSIFIED

Appendix A – Phase 1 Task List

		Task Name	Duration	Start	Finish	Predecess	Resource Names
1		 EDS-P0 IOC	276 days?	Wed 3/1/06	Fri 3/30/07		
2		 Phase 1	276 days	Wed 3/1/06	Fri 3/30/07		
3		 Design BP Prototype	6 days	Wed 3/8/06	Wed 3/15/06		
4		Design layout	5 days	Wed 3/8/06	Tue 3/14/06		PMISE
5		Layout approval by ISC	1 day	Wed 3/15/06	Wed 3/15/06	4	PMISE
6		 Design Branding	6 days	Wed 3/8/06	Wed 3/15/06		
7		Branding white paper	4 days	Wed 3/8/06	Mon 3/13/06		PMISE
8		Branding review by IT	1 day	Tue 3/14/06	Tue 3/14/06	7	PMISE
9		Branding approval by ISC	1 day	Wed 3/15/06	Wed 3/15/06	8	PMISE
10		 Develop BP	14 days	Wed 3/1/06	Mon 3/20/06		
11		Data call	11 days	Wed 3/1/06	Wed 3/15/06		ISC,PMISE
12		HTML complete	3 days	Thu 3/16/06	Mon 3/20/06	5	PMISE
13		Transmit test BP	3 days	Wed 3/15/06	Fri 3/17/06		
14		Transmit BP	1 day	Mon 3/20/06	Mon 3/20/06	11,13	PMISE
15		 Deploy BP	15 days	Wed 3/8/06	Tue 3/28/06		
16		 SCI Domain	15 days	Wed 3/8/06	Tue 3/28/06		
17		Prepare environment	9 days	Wed 3/8/06	Mon 3/20/06		DNI CIO
18		Load test BP	2 days	Tue 3/21/06	Wed 3/22/06	13,17	DNI CIO
19		Load on servers	1 day	Thu 3/23/06	Thu 3/23/06	14,18	DNI CIO
20		Test	3 days	Thu 3/23/06	Mon 3/27/06	18	DNI CIO,PMISE
21		Soft Launch	1 day	Tue 3/28/06	Tue 3/28/06	20	
22		 Secret Domain	15 days	Wed 3/8/06	Tue 3/28/06		
23		Prepare environment	9 days	Wed 3/8/06	Mon 3/20/06		DHS
24		Load test BP	2 days	Tue 3/21/06	Wed 3/22/06	13,23	DHS
25		Load on servers	1 day	Tue 3/21/06	Tue 3/21/06	14,17	DHS
26		Test	3 days	Thu 3/23/06	Mon 3/27/06	24	DHS,PMISE
27		Soft Launch	1 day	Tue 3/28/06	Tue 3/28/06	26	
28		 Validation	7 days	Tue 3/21/06	Wed 3/29/06		
29		 MVT & IT BP Review	6 days	Tue 3/21/06	Tue 3/28/06		
30		Prototype review	1 day	Tue 3/21/06	Tue 3/21/06	5	MVT,IT
31		User validation	1 day	Tue 3/28/06	Tue 3/28/06	20,26	MVT
32		ISC Approval of Phase 1 IOC	1 day	Wed 3/29/06	Wed 3/29/06	31	
33		Phase 1 IOC	0 days	Wed 3/29/06	Wed 3/29/06	32	
34		 Post IOC Tasks	256 days	Wed 3/29/06	Fri 3/30/07		
35		Notification of IOC	0 days	Mon 4/3/06	Mon 4/3/06	33	ISC,PMISE
36		Content Update	256 days	Wed 3/29/06	Fri 3/30/07		
37		 Phase 2 Planning	27 days	Mon 3/13/06	Wed 4/19/06		
38		 Project scope definition	10 days	Mon 3/13/06	Fri 3/24/06		
39		1st Draft Scope & Strategy	5 days	Mon 3/13/06	Fri 3/17/06		PMISE,DNI CIO,DHS
40		1st draft comments	3 days	Mon 3/20/06	Wed 3/22/06	39	IT
41		Final Draft Scope & Strategy -> Specs	2 days	Thu 3/23/06	Fri 3/24/06	40	PMISE
42		 ROM Costs	15 days	Mon 3/27/06	Fri 4/14/06		
43		Data Call	12 days	Mon 3/27/06	Tue 4/11/06	41	PMISE,DNI CIO,DHS
44		Analysis of data to requirements	3 days	Wed 4/12/06	Fri 4/14/06	43	IT
45		 Project plan	13 days	Mon 3/27/06	Wed 4/12/06	38	
46		Draft Project Plan	3 days	Mon 3/27/06	Wed 3/29/06	41	
47		Comments on Project Plan	5 days	Thu 3/30/06	Wed 4/5/06	46	
48		Finalize Project Plan	5 days	Thu 4/6/06	Wed 4/12/06	47	
49		Plan approval by ISC	0 days	Wed 4/19/06	Wed 4/19/06		

Appendix B – High Level Roles and Responsibilities

The Phase 2 IA will develop a more detailed task list as part of the Phase 2 Implementation Plan.

EDS-PO R&R

	Phase 1 (31 Mar 06)	Phase 2 (9-12 months) Bold tasks done during Phase 1	Future Phases Tasks done during Phase 2
PMISE	<ul style="list-style-type: none"> - Draft Blue Pages - Generate Blue Pages Data QA Plan - Draft notification memo - Define "branding" 	<ul style="list-style-type: none"> - EDS-PO Executive Agent - Guide overall efforts; Coordinate IAs - Update Data QA Plan - Generate Customer Outreach Plan - Lead solution development - Report consolidated status to ISC - Validate requirements met 	<ul style="list-style-type: none"> - Incorporate EDS-PO into ISE CONOPS and architecture - Manage per ISE project plan - Define EDS-PO requirements within ISE construct
Host Org (Ph 1) IA (Phase 2)	<ul style="list-style-type: none"> - Deploy Blue Page - Activate web page & links - Coordinate with network owners re usage traffic 	<ul style="list-style-type: none"> - Generate Phase 2 Details <ul style="list-style-type: none"> -- Deliverables -- Cost estimate -- Detail schedule (tests, demos, etc.) - Deploy solution - Report technical performance to PMISE - Coordinate with network owners 	<ul style="list-style-type: none"> - Participate in requirements definition
Implementation Team	<ul style="list-style-type: none"> - Monitor awareness in respective organizations - Increase awareness 	<ul style="list-style-type: none"> - Recommend IAs - Monitor Phase 2 implementation - Identify benefits & impacts - Identify/resolve barriers - Evaluate IOC system extensibility 	
ISC	<ul style="list-style-type: none"> - Approve BP Data QA Plan - Review status - Declare IOC - Approve "branding" 	<ul style="list-style-type: none"> - Approve IAs - Coordinate across Fed govt - Approve updated Data QA Plan - Review status 	<ul style="list-style-type: none"> - Approve EDS-PO requirements
ISC Members (in respective orgs)	<ul style="list-style-type: none"> - Respond to Data Call - Increase awareness 	<ul style="list-style-type: none"> - Promulgate awareness - Ensure data refresh 	
MVT (Mission Verification Team)	<ul style="list-style-type: none"> - Confirm awareness - Assess utility - Recommend EDS-PO "Go-live" 	<ul style="list-style-type: none"> - Assess utility - Verify requirements met - Provide recommendations 	<ul style="list-style-type: none"> - Participate in requirements definition

Appendix C – Data Management & Quality Assurance

Overview of IOC Data Verification

On March 2, 2006, the PMISE issued a data call to participating organizations for contact information for their counterterrorism related offices and watch centers. The PMISE will manually populate the Blue Pages with the content received in response to the data call. Prior to IOC, the PMISE will ask that the Mission Validation Team (MVT) members confirm the data is accurate and ready to be published.

Each ISC member organization will identify a *data quality representative* that will be the primary point of contact with the PMISE for data management issues.

Monthly Data Review

After IOC, the data quality representatives will begin a monthly review of the Blue Pages for accuracy and timeliness. By the close of business on the 4th Friday of each month the data content owners will either 1) provide changes to the PMISE; or 2) email the PMISE indicating that the existing data is current and accurate. The PMISE will update the web content and deliver the updated pages to the hosting organizations (DHS & DNI/IMO) via email. The hosting organizations will then update the production web site within one business day.

Error Correction

To handle ad hoc error notification and correction, the PMISE will insert an email contact link on each web page of the Blue Pages site. Users who notice an error will use the email link to notify the PMISE. After verifying with the content owner's data quality representative that the requested update is valid, the PMISE will make the change and deliver the updated page to the hosting organization for installation on the production site.

ISC Annual Certification

The ISC organization representatives will annually certify that the data their organization owns on the Blue Pages is current and accurate and will notify the PMISE of the certification before March 31st of each year.

Spot Checks

Periodically, the PMISE will perform random checks of the information on the Blue Pages to verify that the contact information is accurate and timely.